3. Enkripsi : Pada saat anda mengubah hurup tersebut dari Arial ke Bookshelf symbol berarti anda sudah melakukan yang disebut System Substitusi ( bukan  Transposisi ) dalam metode Kryptography yang lazim disebut Proses ENKRIPSI ( Encryption ) dengan keyword adalah font Bookshelf symbol , sehingga Surat anda sudah tidak dapat dibaca orang lain.

Dekripsi : Saat anda mengirimkan Surat tersebut dan diterima oleh Pacar anda,  
maka  pacar anda akan mengubah kembali font Bookshelf symbol menjadi Font Arial  agar bisa dibaca kembali. Maka Pacar anda telah melakukan yang disebut Proses Deskripsi ( Descryption ) dengan mengunakan Private Key ( karena dengan kunci yang sama , bukan Public key  ) pada kasus ini keyword nya adalah Font  Arial .

Coding :

Contoh Coding Program

Array 1 Dimensi

#include<constream.h>  
  
  
void main()  
{  
 clrscr();  
 int a[5]={10,15,20,25,30};  
 int b[5]={10,20};  
 int c[5]={15,0,30};  
 int j;  
  
  
 cout<<"\nProgrammer : Singgih Priyanto\n";  
 cout<<"\n";  
 for(j=0;j<5;j++)  
 {  
  cout<<"A ["<<j<<"] = "<<a[j]<<" , B ["<<j<<"] = "<<b[j]<<" , C ["<<j<<"] = "<<c[j]<<endl;  
 }  
 getch();  
}

Encoding : Data file Wave ini dimulai dari offset byte ke-45 dan diambil hanya 10 byte dan dinyatakan dalam heksadesimal.

FF 06 00 FA FF 06 00 7C FE 06

4. Honeypot adalah sebuah sistem pura-pura yang mempunyai service-service yang tidak nyata, dengan vulnerability-vulnerability yang sudah diketahui untuk menarik perhatian para cracker atau mengalihkan mereka dari sistem yang sebenarnya.

6. Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

7. Komputer forensik yang juga dikenal dengan nama digital forensik, adalah salah satu cabang ilmu [forensik](http://id.wikipedia.org/wiki/Forensik" \o "Forensik) yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan dijital.

Tujuan dari komputer forensik adalah untuk menjabarkan keadaan kini dari suatu artefak dijital. Istilah artefak dijital bisa mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, hard disk, atau CD-ROM), sebuah dokumen elektronik (misalnya sebuah pesan email atau gambar JPEG), atau bahkan sederetan paket yang berpindah dalam jaringan komputer.

8. Di bidang Disk Forensik, dapat dilacak kapan sebuah data dihapus, di modifikasi ataupun dapat mengembalikan password yang hilang, data yang hilang dan sebagainya. Ataupun melihat transaksi yang sedang berlangsung dalam sebuah jaringan komputer dan lain-lain. Semua hal tersebut dapat dilakukan dengan memanfaatkan beberapa tool pendukung, baik berupa software maupun hardware.

9. Keamanan jaringan ([Bahasa Inggris](http://id.wikipedia.org/wiki/Bahasa_Inggris" \o "Bahasa Inggris): Network Security) dalam [jaringan komputer](http://id.wikipedia.org/wiki/Jaringan_komputer" \o "Jaringan komputer) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan.

Segi-segi keamanan didefinisikan dari kelima point ini.

a. Confidentiality Mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.

b. Integrity Mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.

c. Availability Mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.

d. Authentication Mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu. e. Nonrepudiation Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Serangan (gangguan) terhadap keamanan dapat dikategorikan dalam empat kategori utama :

a. Interruption Suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

b. Interception Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.

c. Modification Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

d. Fabrication Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.

10. Sebuah **botnet** adalah sekumpulan program yang saling terhubung melalui [Internet](http://id.wikipedia.org/wiki/Internet) yang berkomunikasi dengan program-program sejenis untuk melakukan tugas tertentu. Botnet bisa dipakai untuk menjaga keamanan kanal [IRC](http://id.wikipedia.org/wiki/IRC), mengirimkan surel spam, atau berpartisipasi dalam serangan [DDos](http://id.wikipedia.org/w/index.php?title=DDos&action=edit&redlink=1" \o "DDos (halaman belum tersedia)). Kata botnet berasal dari dua kata, [*robot*](http://id.wikipedia.org/wiki/Robot) dan [*network*](http://id.wikipedia.org/wiki/Jaringan_komputer).

Botnet dieksploitasi untuk berbagai keperluan, antara lain [serangan DoS](http://id.wikipedia.org/wiki/Serangan_DoS" \o "Serangan DoS), penciptaan atau penyalahgunaan [relai surat SMTP](http://id.wikipedia.org/wiki/SMTP" \o "SMTP) untuk spam (lihat [Spambot](http://id.wikipedia.org/w/index.php?title=Spambot&action=edit&redlink=1" \o "Spambot (halaman belum tersedia))), [pemalsuan klik](http://id.wikipedia.org/w/index.php?title=Pemalsuan_klik&action=edit&redlink=1" \o "Pemalsuan klik (halaman belum tersedia)), [spamdeks](http://id.wikipedia.org/w/index.php?title=Spamdeks&action=edit&redlink=1" \o "Spamdeks (halaman belum tersedia)), dan pencurian nomor serial aplikasi, [identitas masuk log](http://id.wikipedia.org/w/index.php?title=Masuk_log&action=edit&redlink=1" \o "Masuk log (halaman belum tersedia)), dan informasi keuangan seperti [nomor kartu kredit](http://id.wikipedia.org/w/index.php?title=Nomor_kartu_bank&action=edit&redlink=1" \o "Nomor kartu bank (halaman belum tersedia)).

Komunitas pengendali botnet sudah lama berjuang memperebutkan gelar pemilik bot terbanyak, pita lebar tertinggi, dan mesin terinfeksi paling "berkualitas tinggi", seperti universitas, perusahaan, dan pemerintahan